

ENDURING VALUES. INSPIRED PERFORMANCE.®



SOCIAL NETWORKING – Unsafe at Any Speed?

Carl Willis-Ford
Senior Principal – Solution Architect
ISSA Senior Member
FISSEA Technical Working Group





Speaker Background

- Senior Principal – Solution Architect for CSRA, Inc.
- 8 years U.S. Navy, nuclear reactor operator, fast attack submarines
- Over 25 years experience: data management, IT process, technical management, information security
- B.S. Computer Science (1993)
- M.S. Network Security (2006)
- M.S. Technology Management (2008)
- CIO University Certificate (Federal Executive Competencies), GSA/CIOC (2008)
- Adjunct Faculty, George Mason University School of Business
 - Technical Project/Portfolio Management, Grad/Undergrad
 - Networks & Security, Undergrad
- Doctorate in Information Assurance, expected 2018
- Senior Member, Information Systems Security Association

Social Network

- From Dictionary.com:
 - a network of friends, colleagues, and other personal contacts:
 - an online community of people with a common interest who use a website or other technologies to communicate with each other and share information, resources, etc.:
 - a website or online service that facilitates this communication.



Find us on:
facebook®

Social Network Variety



The Most Popular



- General Interest
 - 1.1B unique visitors/month



- 240 characters per message



- The social network for business



- Sharing images/videos



- Google's competition for Facebook



- Cross between Facebook and a blog. Sharing



- Sharing images/videos



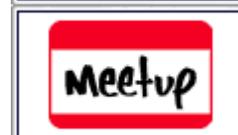
- Europe's largest general social networking site



- Started as image hosting, added social networking



- Share 6 second video clips



- Advertise local group meetings



- Focused on quickly meeting others with same interests



- Anonymously ask/answer questions



- Focus on finding new people to chat with online



- Focus on finding/connecting with former classmates

Plenty of Newer/Smaller Social Networks



...and hundreds more

What do
we do?



So...How Do We Talk to People about Social Networks?

- Just Say **NO** ?
 - Some security experts recommend avoiding social networks
- However
 - LinkedIn for hiring/job searches/work-related communities
 - Facebook for staying connected with family/friends
 - Share photos, recipes, poetry, videos, 3D models, etc.
 - Many companies use social media as part of their marketing strategy
- So – how real is it to expect people to stay away from Facebook?
 - (remember...1.1 Billion unique visitors/month)
- So, just say **Be Careful** ?? We need more.

Don't Over Dramatize

- Talk about Risks



- Be realistic about Impacts
- If you can't explain impacts, they won't listen
- Talk about how to manage Risks
 - Simple guidance
 - Show how to manage security settings





Possibly Hyped Risk Examples

- How realistic is it to expect to be stalked via social networks by a stranger?
 - From 2012 DoJ report:
 - 1.5% of population 18 or older were victims of any type of stalking during the 12 month measurement window
 - 70% of them knew their stalker
- How likely is it to have your identity stolen through social networks?
 - Top sources of Identity Theft (no particular order)
 - Social Engineering, including
 - Phishing
 - Phone spoofing
 - Dumpster diving
 - Data breaches
 - Stealing credit card, wallet, purse
 - Skimming
 - Shoulder surfing



Real Risks!

Viral Quizzes (Facebook)

- Many different examples
 - What state do you belong in?
 - What Harry Potter character are you?
 - What Classic Rock Band are you?
- Quizzes are often hosted by 3rd party site
 - Collects answers, tied to your Facebook account
 - Answers shared (sold) to advertisers
 - Answers may include common password reset information
 - Name of first pet
 - Street where you grew up
 - First car (make/model)



I'll take it...

WHAT CAR SHOULD YOU DRIVE?

START!

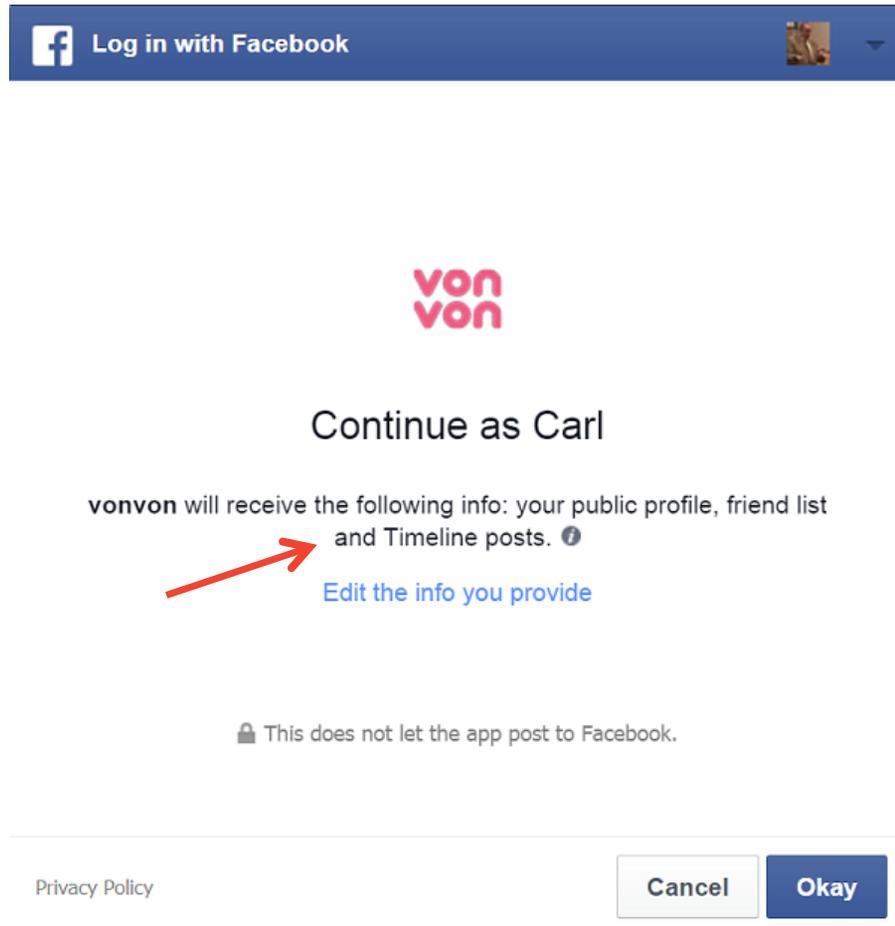
I got Bugatti Veyron. What car should you drive?

You live a bit luxuriously and quality means everything to you. You also realize it's not really about impressing others but never being disappointed for yourself. Being top-notch is an innate part of you and it's almost disingenuous to suppress that....

BITECHARGE.COM

Like · Comment · Share

Facebook Apps



Log in with Facebook

von von

Continue as Carl

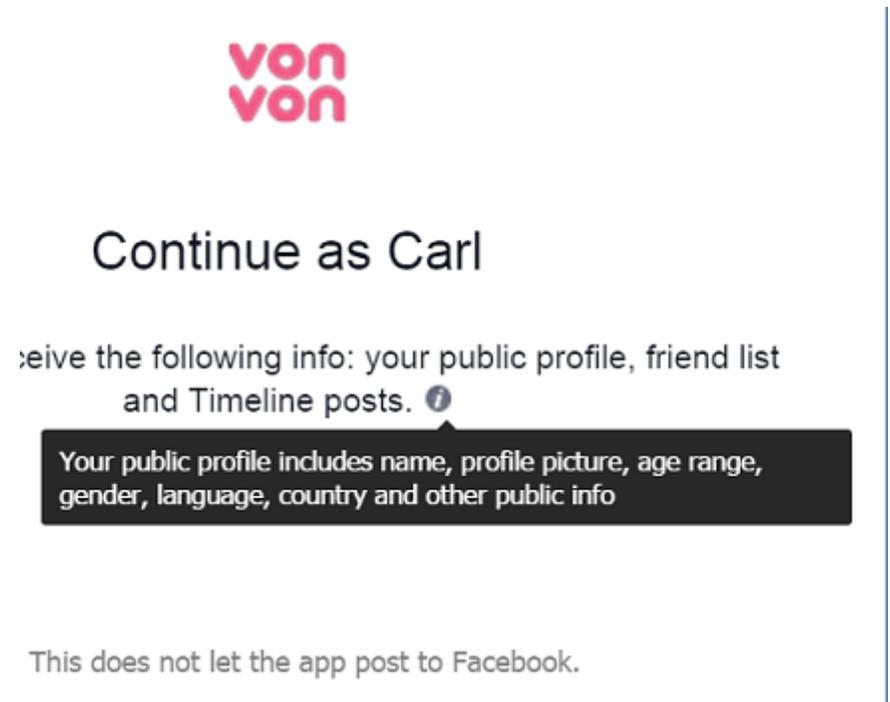
vonvon will receive the following info: your public profile, friend list and Timeline posts. ⓘ

[Edit the info you provide](#)

🔒 This does not let the app post to Facebook.

Privacy Policy

Cancel Okay



von von

Continue as Carl

Receive the following info: your public profile, friend list and Timeline posts. ⓘ

Your public profile includes name, profile picture, age range, gender, language, country and other public info

This does not let the app post to Facebook.

Install this 'game', and VonVon will be seeing all of your posts, even if only shared with friends...

Free Stuff! (Facebook)



- Shared from a friend, seems easy to get something for nothing



Vouchers Remaining: -5776

Step 1. Share This Page

Share 350

Step 2. Comment "Thank You!"

210 comments

Add a comment

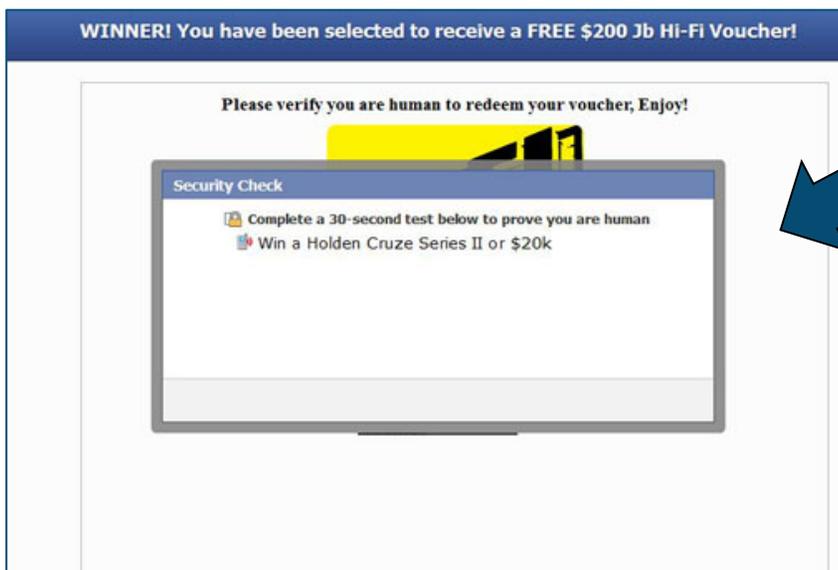


Thank you!

Reply · 1 Like · Follow Post · 11 minutes ago

View 209 more

Facebook social plugin



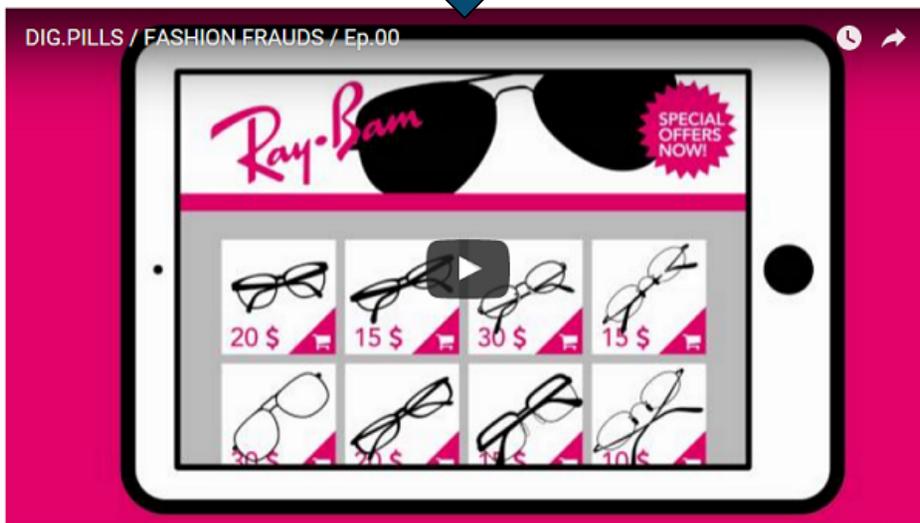
- When you click, you're sent to a survey site, asked questions to get personal information
 - Email, phone, address
 - At a minimum, set up for spam

More free/low price stuff! (Facebook)

- 'Free' trip survey scam



- Knock-off products



(clicking the link does NOT take you to Ray-Ban)

Carnival Cruises
January · 🌐 · 📷

Like Page

Surprise your family/kids by winning a Carnival Cruise
(Limited Time)

January

Just share this post then go here: [redacted] for a chance of winning up to 5 tickets for a Carnival Cruise. Winners are notified. Like our page for updates. Good Luck!

Looking for services? Don't look here...

- Looking for a moving company
 - Used Facebook
 - Moving company took their stuff
 - Never showed up again



<http://www.telegraph.co.uk/news/uknews/crime/11901286/Couple-lose-almost-everything-after-Facebook-removal-van-scam.html>



Friend Requests (All)

- SOCIAL ENGINEERING
- Getting connect requests from people you don't know
 - No (or very few) mutual friends
 - No past connection to them
 - Setting you up for scams on Facebook
 - Later claim to be Facebook staff and...you've won a prize!
 - But you have to send \$\$ in order to collect
 - Collecting personal information via chat/messaging
 - Spam
 - Password reset questions
 - Information harvesting on LinkedIn and others
 - Asking for personal information
 - Asking for business-sensitive information

Robin Sage



Do you know this woman?

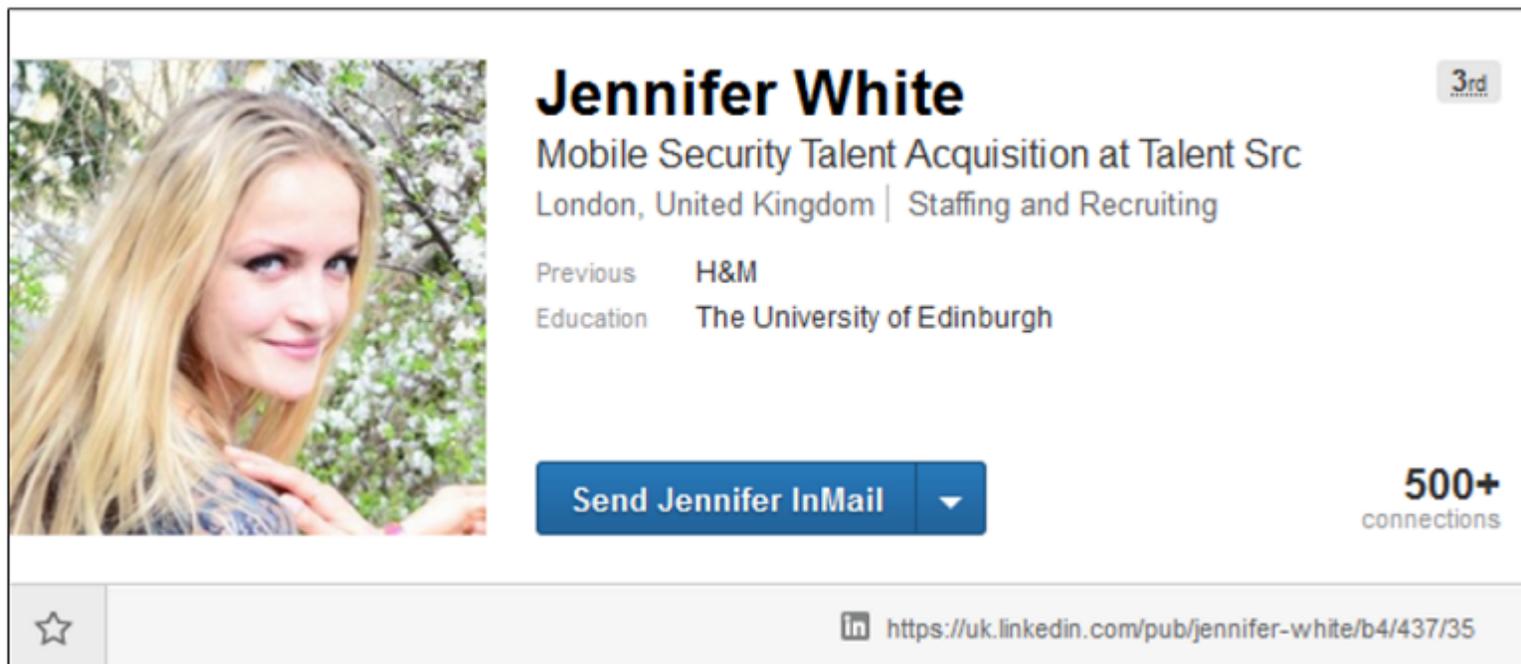
...she wants to be your friend



Robin Sage Experiment

- December 2009 to January 2010
- Fake Facebook, Twitter, LinkedIn profiles, posing as a Cyber Threat Analyst
- Sent requests and established social network connections with over 300 security professionals
 - Men and women of all ages
 - NSA, DoD, and Global 500 companies
- Results
 - Deployed troops discussing locations and movement
 - Consulting opportunities from Lockheed Martin and Google
 - Given business sensitive documents for review
 - Able to determine answers to password change questions based on information provided in online conversations

Fake Recruiter Data Mining - 2015



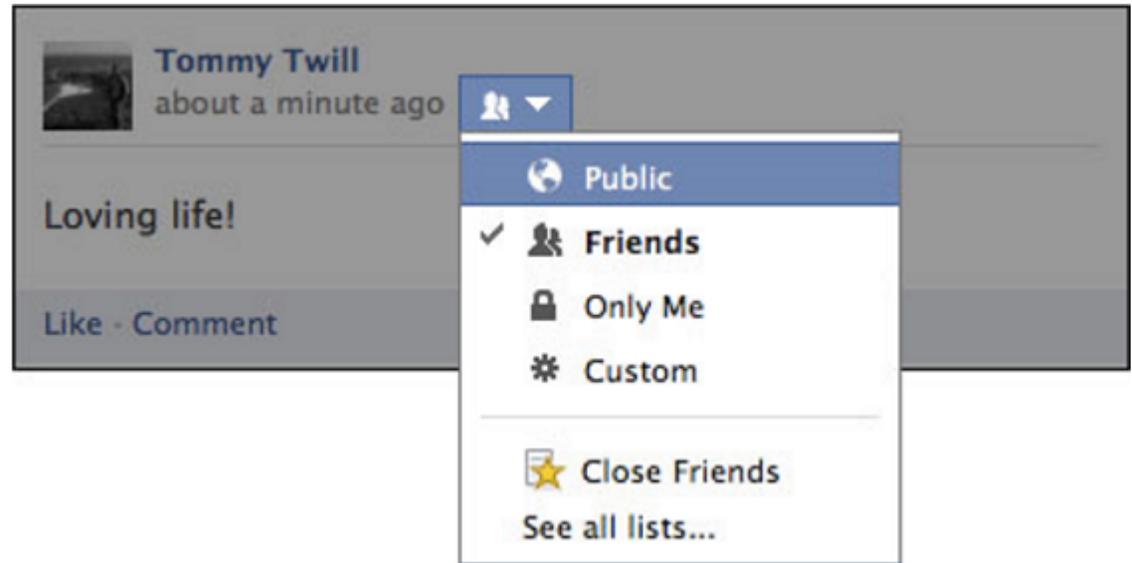
The screenshot shows a LinkedIn profile for Jennifer White. On the left is a profile picture of a young woman with long blonde hair. To the right of the photo, the name "Jennifer White" is displayed in large bold text. Below the name, the current position is listed as "Mobile Security Talent Acquisition at Talent Src" in London, United Kingdom, with the industry "Staffing and Recruiting". Previous employers are listed as "H&M" and education as "The University of Edinburgh". A blue button labeled "Send Jennifer InMail" is visible. In the top right corner of the profile header, it says "3rd" with a small icon. In the bottom right corner, it says "500+ connections". At the bottom of the profile header, there is a star icon on the left and a URL "https://uk.linkedin.com/pub/jennifer-white/b4/437/35" on the right.

- Company logo a generic graphic
- 24 recruiters, each with different specific cyber specialty
 - Recruiter pictures also generic, found elsewhere on internet
 - Reverse image searches of mirror-flipped photos
- Mapping infosec people's networks – not sure why



Advice for Users

General Tips



- Always check who you are sharing things with
 - Most networks allow setting a default for all posts
 - Facebook restricts photos/videos to your original audience, even if someone re-shares
- When you share a photograph that you took, you also share the EXIF (location, date/time) data. Facebook automatically strips this, but not all social networks do that.

General Tips, continued

- Think about what you are sharing...don't overshare
 - 'Going on vacation for two weeks'
 - Will be out of touch
 - Can someone watch our house for us?
 - Do you know who all your friends are?
 - Personal, embarrassing information about yourself or your family/friends
- Don't get into 'flame' wars
 - People more willing to do via Facebook than face-to-face
 - Wear your armor...don't be goaded into angry replies
- Keep work and private life separate in social media
 - Separate Twitter accounts, one for work, one for personal
 - Keep personal out of LinkedIn

Facebook Burglary

Rare
(not unheard of)

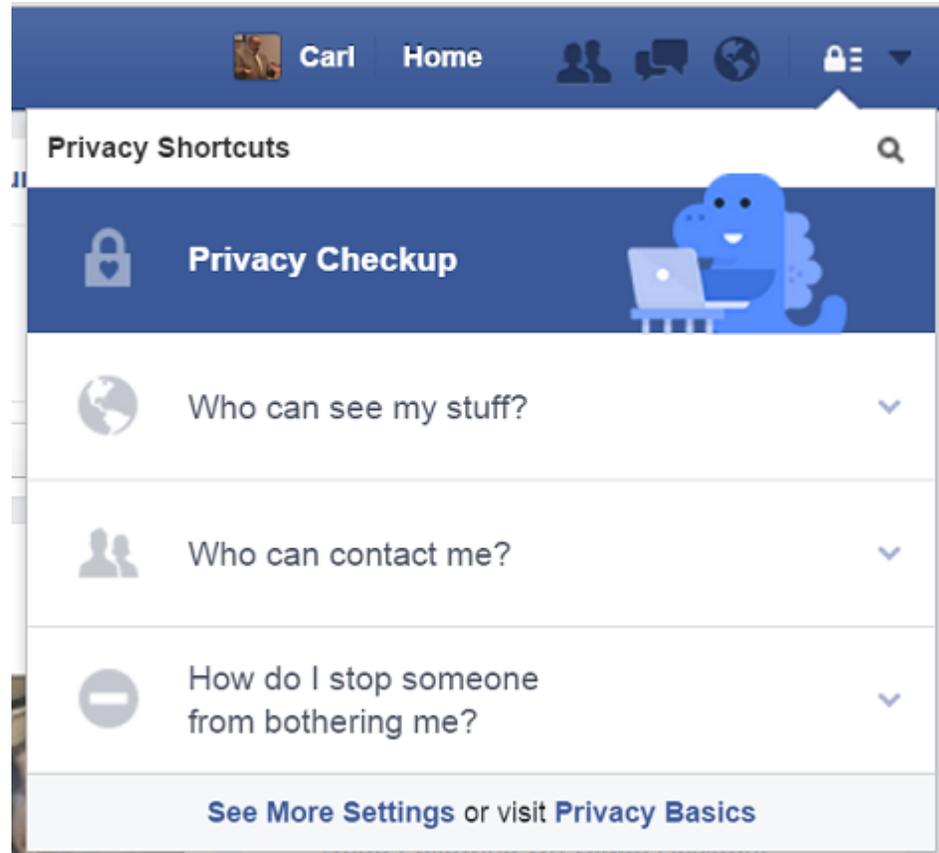


Careful where you Click!!

- Like Farming
 - Facebook photos that show dogs with signs around their neck
 - ‘Teachers’ holding signs asking you to Like and share to show their students how things go viral
 - A kid with a sign saying that 100,000 likes will cause his father to stop smoking
 - **Mostly harmless**, but used for gathering clicks (popularity) which is Facebook currency...they replace the original content with a scam-ad, but keep all the likes so that it gets prominent placement.
- Click Bait
 - If it looks too good to be true, and you don’t know the original poster (a friend may have shared it).
 - Used for:
 - Downloading malware or sending you to a scam ad
 - Farming to raise popularity

Manage Security & Privacy - Facebook

- You can find the Privacy Checkup here...



Manage Security & Privacy - Facebook

Privacy Checkup

Thanks for making some time for this. Now let's go through 3 steps to help make sure you're sharing with the right people.



1 Posts

Whenever you post from News Feed or your profile, you can choose an audience to control who sees it.

Who do you want to see your next post?

Tip: You can change your audience each time you post.

[Learn More](#) [Next](#)

2 Apps

3 Profile

Manage Security & Privacy - Facebook

2 Apps

Here are apps you've used Facebook to log into. Go ahead and edit who sees each one and delete any you don't want anymore.

Tip: You can always edit your apps later from your [app settings](#).

 Waze	 Only Me ▾	
 Makeblock Forum		
 Imgur		
 Meetup		
 Eventbrite	 Only Me ▾	

-  Public
-  Friends
-  Only Me
-  Custom
-  More Options

Learn More

Next



Biggest Risks for Companies

- Employees sharing too much information
- Loss of confidential/business sensitive information
- Increased exposure to litigation
- Loss of employee productivity
- Increased exposure to malware



Social Networking at Work

- Be mindful of agency/company policy for social networking
 - You are responsible for knowing policy
- Don't accidentally take on the role of agency spokesperson
- Are you allowed on social networks from work?
 - LinkedIn?
 - Facebook?
 - Yelp?
 - TripAdvisor?
 - None of them?
- Are you allowed to share work events on your social network?
 - Employees sharing bosses promotion before announced
 - Posting cellphone pictures/videos taken at the office
 - Some co-workers may not want their image on your social network
- Maybe point them to the policy?



References

- <https://staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks>
- http://lancasteronline.com/features/how-it-s-done-internet-quizzes-may-collect-more-than/article_c58e438a-9b2b-11e3-8304-001a4bcf6878.html
- <http://www.cnet.com/how-to/how-to-enable-two-factor-authentication-on-popular-sites/>
- Stalking
- http://www.bjs.gov/content/pub/pdf/svus_rev.pdf
- Social Network Identity Theft
- <http://www.idtheftcenter.org/Fact-Sheets/fs-138.html>
- <http://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm>



References

- Social Network Site Security
 - [https://help.linkedin.com/app/answers/detail/a_id/267/~account-security-and-privacy---best-practices](https://help.linkedin.com/app/answers/detail/a_id/267/~/account-security-and-privacy---best-practices)
 - <https://www.facebook.com/help/379220725465972>
 - <https://support.twitter.com/articles/76036>
 - <https://security.google.com/settings/security/secureaccount> (security checkup)



Thank You

Questions?